Information Sharing Strategies of the United States Federal Government and Its Allies and Our Contributions Towards Implementing these Strategies

Version I

Technical Report UTDCS-23-10
Department of Computer Science
The University of Texas at Dallas
August 2010

Dr. Bhavani Thuraisingham

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Sharing Strategies of the United States Federal Government and Its Allies and Our Contributions Towards Implementing these Strategies Version 1	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **University of Texas at Dallas,Department of Computer Science,Richardson,TX,75083**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report provides a survey of the major initiatives within the US Federal Government in Information Sharing. In particular, we discuss information sharing strategies and initiatives within the Department of Defense, Department of Justice Department of Homeland Security, and Director of National Intelligence. In addition we also discuss some of the initiatives within agencies such as the Department of Health and Human Services, as well as some of the international efforts within the United Kingdom and Australia. This report was prepared as part of the AFOSR MURI project on Assured Information Sharing. A deliverable under this project is to monitor the strategies of the US Federal Government and its allies so that we can develop effective solutions to the major problem of information sharing critical to fight the global war on terror. This report will be updated as progress is made on information sharing within the federal agencies in the United States and in the allied nations.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**20**	

Information Sharing Strategies of the United States Federal Government and Its Allies and Our Contributions Towards Implementing these Strategies Version 1

Dr. Bhavani Thuraisingham
The University of Texas at Dallas

August 2, 2010

ABSTRACT

This report provides a survey of the major initiatives within the US Federal Government in Information Sharing. In particular, we discuss information sharing strategies and initiatives within the Department of Defense, Department of Justice, Department of Homeland Security, and Director of National Intelligence. In addition, we also discuss some of the initiatives within agencies such as the Department of Health and Human Services, as well as some of the international efforts within the United Kingdom and Australia. This report was prepared as part of the AFOSR MURI project on Assured Information Sharing. A deliverable under this project is to monitor the strategies of the US Federal Government and its allies so that we can develop effective solutions to the major problem of information sharing critical to fight the global war on terror. This report will be updated as progress is made on information sharing within the federal agencies in the United States and in the allied nations.

DISCLAIMER: Unless otherwise stated, the views and conclusions described in this report are those of the author and do not reflect the policies and procedures of the University of Texas at Dallas, the Air Force Office of Scientific Research or the United States Government.

1. INTRODUCTION

Daniel Wolfe (formerly of the NSA) defined assured information sharing (AIS) as a framework that "provides the ability to dynamically and securely share information at multiple classification levels among U.S., allied and coalition forces." As stated in the DoD information sharing strategy document, the DoD's vision for AIS is to "deliver the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment". Our objective is to help achieve this vision by defining an AIS lifecycle and developing a framework to realize it.

To address the information sharing strategy of the DoD, we are conducting research on this topic under an AFOSR MURI project. Our research is framed by a set of AIS

requirements relevant to applications found in the DoD, government and industry. The significant research contributions of our project will include the definition of an AIS Lifecycle (AISL) that is driven by the 4Vs (*volume, veracity, velocity, vector*) as well as cross-cutting requirements and the development of (1) a framework based on a secure semantic event-based service-oriented architecture to realize the life cycle, (2) novel policy languages, reasoning engines, negotiation strategies, and security infrastructures, (3) techniques to exploit social networks to enhance AISL, (4) techniques for federated information integration, discovery and quality validation, and (5) techniques for incentivized assured information sharing. The research is carried out by a coalition of six institutions: The University of Maryland, Baltimore County (SOA, Semantic Web), Purdue (Policies and Security), The University of Texas at Dallas (Incentives and Knowledge Management), University of Illinois Urbana Champaign (Information Management), The University of Texas at San Antonio (Policy and Applications) and the University of Michigan (Social Networks).

Since we proposed the effort in October 2007 and started the project in mid 2008, a lot of initiatives have been proposed on AIS by the US Government and its allies. In addition, the DoD also published its Information Sharing Implementation Plan in April 2009. Other notable efforts include the Department of Justice Information Sharing Initiative, the Department of Homeland Security Information Sharing Strategy and the Office of National Intelligence Information Sharing Strategy. In this report, we will summarize the various efforts of the US Government on information sharing. With respect to our efforts, we now have international partners (Kings College, London and University of Insubria, Italy). We also have a sister project funded by AFOSR on secure cloud computing that is developing secure infrastructures and data managers for clouds (The University of Texas at Dallas and Purdue). As part of the joint initiative between the two projects, we are demonstrating assured information sharing in a cloud environment with our international partners.

This report is an evolving document and will be updated periodically. Our MURI project will review the information in this document and will enhance its current research efforts based on guidance provided by the DoD and other agencies. The organization of this document is as follows. Section 2 discusses general issues in assured information sharing. DoD's information sharing strategy and implementation plan will be discussed in Section 3. Justice Information Sharing Initiative including its NIEM (National Information Exchange Model) will be discussed in Section 4. DHS information sharing strategy will be discussed in Section 5. Office of National Intelligence information sharing strategy will be discussed in Section 6. National Information Sharing Strategy proposed by the White House to (coordinate the efforts of the DoD, DOJ, IC, and DHS as well as the efforts of the International partners) will be discussed in Section 7. Efforts of the Department of Health and Human Services as well as other US Government efforts will be discussed in Section 8. International efforts will be discussed in Section 9. Our views will be discussed in Section 10.

2. SUPPLY CHAIN MODEL FOR ASSURED INFORMATION SHARING

As stated in Section 1, to fight the global war on terror, organizations have to share data but at the same time enforce appropriate policies. We need to understand clearly what it means to migrate from a need to know to a need to share paradigm. Even if the culture is moving toward need to share, we still have to protect the critical assets of

the nation. Therefore, we need to enforce appropriate policies and procedures. We have drawn an analogy between information sharing and the theory of supply chain management. The partners in producing a data product need to have common incentives, share the risks, and work towards producing the best product possible but at the same time ensure the individual autonomy.

Our goal is to develop a data supply chain model to develop data products that can be shared among the agencies/coalition partners. That is, each data product is developed according to the rules of a data supply chain model. In order for a successful data chain-based approach, the partners of the supply chain also have to share the information, risks and costs. Furthermore, the incentives have to be aligned every step of the way. This means that the approaches used in supply chain management have to be examined for data supply chain management. In addition, several information management technologies play an important role.

Suppose a customer needs a data product. The first step is to determine who to go to to get the data. This means we need metadata that will guide us in getting the locations of the individuals who possess the raw materials (i.e. the raw data). The raw data will be in data sources. The next step is to determine how to get the data from A to B in the form we need. What are the transformations to the data? What path should the data take? How is the data stored at the intermediate locations? Technologies that we need for this process are (i) integration of heterogeneous data sources (ii) cleaning the data every step of the way (iii) understanding the provenance of the data (iv) enforcing appropriate polices – e.g. is the combined data at a higher classification level than the individual pieces of the data?, and (vi) extracting the data that is needed for the processing of the data at every stage.

Conducting this entire process in real-time is a challenge. Therefore, concepts from the raw data such as email, chats, blogs, web pages and social media pages have to be extracted and linked to for networks. This process has to be carried out continuously so that if and when a customer needs a data product, many of the components are already there. This is similar to using existing raw material for a product rather than trying to develop new raw material. The linked data also has to be analyzed so that the nuggets are produced for effective knowledge management of a corporation or an agency. Therefore, some of the key technologies include semantic web for representing the vast amount of heterogeneous data, data mining for extracting concepts from the data, network analysis, and knowledge management.

Another challenge is to get the right amount of the right parts at the right time to the consumer. That is, if the parts do not arrive on time, then the supply chain process will be disrupted. Also, if there are too many parts supplied (i.e. too much inventory) then it will be very costly. We have heard about the CISCO situation when the company lost several millions of dollars due to too much inventory. Therefore, we need appropriate inventory management techniques. This is also the situation for data. We need the right data at the right time to go to the right place. If the data does not arrive on time, then there will be a delay introducing the final product and this delay could be not just costly but also deadly. Similarly, if there is too much data, then the consumer has to sort the data and extract only the relevant data to complete the data product.

In summary, here are the parallels between data supply chain and regular supply chain. At the lowest level in the data side, you have raw data such as emails and blogs; in the regular supply chain side, you have the nuts, bolts, cement (in the case of

building say a house). At the intermediate level, you have the network in the data side which will include the nodes and links extracted from the raw data. At the supply chain side you have the doors, windows, and the foundation among other things. At the finish line on the data side, you have the complete data product which could be the negates (i.e., knowledge) extracted from the networks. At the regular supply chain side, you have the complete house. At every step there are policies. For the data side, you have confidentiality policies, integrity policies and administrative policies. At the supply chain side, you have the regulations and guidelines to building a house.

3. DEPARTMENT OF DEFENSE

2.1 Overview

Department of Defense has published two significant documents in information sharing. In May 2007, the Assistant Secretary of Defense and the DoD Chief Information Office (Hon. John Grimes) published the DoD Information Sharing Strategy. Our MURI proposal, which was written in October 2007, closely followed the guidance provided by the DoD in its Information Sharing strategy document. Then in April 2009, the Office of the Assistant Secretary of Defense published the DoD Information Sharing Implementation Plan. Much of our work in the MURI enhances and augments the implementation plan that has been put forward by the DoD. For more details we refer to the project website [AISL].

In Section 2.2, we will summarize the DoD Information Sharing Strategy and in Section 2.3, we will summarize the DoD Information Sharing Implementation Plan. As new information becomes available, we will update this document on information sharing strategies of the US Federal Government.

2.2 DoD Information Sharing Strategy

In May 2007, the DoD CIO published a document [DOD1] that articulated DoD's Information Sharing Strategy. The vision for information sharing is to "develop the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment". To achieve this vision, the DoD has formulated the following four goals: (i) "Promote, encourage and incentivize sharing", (ii) "Achieve an extended enterprise", (iii) "Strengthen the agility in order to accommodate unanticipated partners and events", and (iv) "Ensure trust across organizations". DoD has stated that the four information sharing goals will be realized through five approaches. Our strategy on our MURI project is to develop solutions to implement these five approaches (Finin, 2009). These approaches are the following:

1. ***Recognize & leverage the Information Sharing Value Chain. "****The Information Sharing Value Chain articulates the 'opportunity' of information sharing to support informed decision making, shared situational awareness and improve knowledge at every level of the DoD. The risks encountered at each step of the information sharing value chain must be managed to mitigate negative consequences*." We are developing a framework for Assured Information Sharing Lifecycle to address this approach.

2. ***Forge information mobility.*** "*Information mobility is the dynamic availability of information which is promoted by the business rules, information systems, architectures, standards, and guidance/policy to address the needs of both planned and unanticipated information sharing partners and events. Information mobility provides the foundation for shared and user-defined situational awareness. Trusted information must be made visible, accessible, and understandable to any authorized user in DoD or to external partners except where limited by*

law or policy." Our solution to this approach is to develop architectures, policies, and secure social networking, as well as share our findings with the Air Force Knowledge Management program.

3. ***Make information a force multiplier through sharing. "****Information as a force multiplier refers to exploiting relative information advantages against our adversaries and to support effective, unified disaster response. Sharing is inherent in information becoming a force multiplier and results in increased operational effectiveness."* Our solution to this strategy is to design and implement modules for information integration, analysis and quality management that address the 4Vs – Volume, Veracity, Velocity and Vector.

4. ***Promote a federated Information Sharing Community/Environment. "****Governance, policy and cultural considerations establish the required multi-lateral relationships working in a regulated, risk management environment that ensures information security, privacy, and trust. The federated approach establishes and maintains a trusted community of information sharing that promotes collaboration, leverages the information integrators in the community and reduces the "seams" between organizations, domains and functions.*" Our solution to this approach is to share our research on federated information integration and policy management with DoDAF (DoD Architecture Framework).

5. ***Address the economic reality of information sharing. "****Create guidance and incentives within the budgeting and resource allocation process to encourage organizations to share information that promotes informed decision making, improves situational awareness, establishes economies of knowledge, and creates unity of effort.*" Our solution to this approach is to develop theories and tools for behavior-based incentivized assured information sharing.

DoD's Information Sharing Strategy document also discusses implementation considerations. In particular, the DoD states that five cross-cutting areas called the five key touchstones are: Culture, Policy, Economic Resources, Governance, Technology and Infrastructure. Essentially, the DoD states that there has to be a culture switch so that information sharing is promoted and encouraged. Policies, procedure and guidelines have to be in place to guide sharing. Governance stature has to be established, Incentives will be taken into consideration in the building and resource allocation process. Finally, the DoD will leverage its many investments in building technologies and infrastructures and make new investments to support the net-centric environment. We believe that (i) the technologies we are developing in our MURI project, (ii) the breakthrough incentive-based information sharing approaches we are developing, and (iii) the cloud computing infrastructures embraced by the DoD will significantly contribute toward solutions for information sharing. In the next section, we will discuss the implementation plan for information sharing that was published by the DoD in April 2009.

3.3 DoD Information Sharing Implementation Plan

The DoD Information Sharing Implementation plan [DOD2] has identified ten focus areas to implement the strategy discussed in Section 2.2. In each of the focus areas, the implementation plan gives an overview of the area, the tasks to be carried out, the details of the tasks and the DoD organization responsible for implementing the tasks. The tasks are identified by the Office of the Secretary of Defense, the combatant commands, military services and defense agencies (called CC/S/A). In this section, we will summarize the focus areas and list the tasks. For more details, we refer to (DoD, 2009). We will also discuss how we are addressing the various focus areas in our project.

Focus Area 1: Managing Information Sharing in the DoD

It is stated that the DoD must share infrastructures in a timely manner not only with the war fighters but also with other agencies for intelligence, counter-terrorism and

stability operations. Therefore, coordination is critical. To ensure coordination, the DoD states that a governance structure must be established.

> "*Task 1.1 Establish an overarching governance structure for DoD enterprise information sharing.*
>
> *Task 1.2 Develop and manage information sharing situation awareness to ensure synchronization among activities*."

Focus Area 2: Installing an Information Sharing Culture

It is stated that the DoD and other agencies are moving toward an information sharing paradigm. In particular, the DoD is moving from a parochial culture to collaborative development though various initiatives. For example, in addition to forming Communities of Interests (COI), the North American Airspace Defense Command (NORAD) and the United States Northern Command (USNORTHCOM) are using Information Exchange Brokers for information sharing and knowledge management.

> *"Task 2.1 Develop incentives to promote information sharing practices and procedures.*
>
> *Task 2.2 Identify and revise the policies and processes that create impediments or disincentives to sharing information while ensuring the Department's continued compliance with laws, policies and agreements.*
>
> *Task 2.3 Educate and train personnel on their roles in information sharing.*
>
> *Task 2.4 Determine the applicability of and expand if validated the NORAD/USNORTHCOM IEB concept to other CC/S/As to enhance organizational information exchange processes and procedures."*

Focus Area 3: Leveraging the Power of Social Networks

DoD is promoting social networking among its personnel by providing them with tools and technologies. For example, the DKO (Defense Knowledge Online) has enabled the DoD community to use shared spaces, provided them with tools for information sharing and best practices. However, DoD has some concerns about its personnel using public social networking websites due to security concerns. Therefore, the risks associated with the social networks have to be taken into consideration.

> *"Tasks 3.1 Develop a plan to leverage modern social networking capabilities appropriately within the DoD."*

Focus Area 4: Operationalizing Information Sharing

It is stated that information sharing is critical for mission success. Therefore, it has and will continue to carry out joint exercises and demonstrations with respect to information sharing to determine the gaps and opportunities. Examples include the Coalition Warrior Interoperability Demonstration (CWID) which the USNORTHCOM hosted for homeland defense.

> *"Task 4.1 Develop an approach that ensures information sharing activities (policies, procedures, and technologies) are integrated into appropriate joint experiments, demonstration, and exercises."*

Focus Area 5: Removing Sharing Barriers created by Improper Classification

Appropriate classification of national security information is critical to protect the information and safeguard the nation. However, it is stated that the overclassification of information will also be a barrier to national security. This is because the right information may not arrive at the right time due to extensive security controls. Therefore, the implementation plan states that automated tools for properly

classifying the information are needed.

> *"Task 5.1 Coordinate with ODNI to update 'write-for-customer resource' guidance and 'write-for customer relevance' and terrorism information sharing training for all partners.*
>
> *Task 5.2. Coordinate with ODNI and the Information Security Oversight Office to update information sharing policy, guidance and training materials."*

Focus Area 6: Sharing Unclassified Information for Civil Support and SSTR Operations

DoD's goal is to also support civilian missions including disaster recovery and health epidemics. Recent efforts included the response to Hurricane Katrina. In this situation, it is vital that unclassified information be shared securely. DoD also provides support to US foreign stability, security, transition and reconstruction (SSTR) operations. And information sharing among the right people and the right time is important for such civilian missions. It is stated that that many of the U.S. combatant commands have established portals for information sharing including United State Joint Forces Command's (USJFCOM) Harmoniweb.

> *"Task 6.1 Develop an enterprise approach, informed by the USJFCOM-led MNIS (Multinational Information Sharing) Analysis of Alternatives (AoA) that enables the federation of existing CC/S/A unclassified information sharing systems in support of civil support and SSTR operations."*

Focus Area 7: Sharing Information for Enhanced Operations

It is stated that mission partner information sharing is to be the number one priority of the combatant commands. Yet, at present, each combatant command uses its own technologies and infrastructures. The end result is a proliferation of networks and infrastructures. It is therefore important that the SOA-based Global Information Grid information assurance capabilities are provided in the national networks and the networks shared with the coalition partners.

> *"Task 7.1 Develop an architecture to converge the multiple secret level coalition networks into a single mission partner assured information sharing environment, providing a common suite of information services to all mission partners, along with controlled access to command and control as well as intelligence applications in support of mission planning and execution based on the trust level and duties of the individuals user."*

Focus Area 8: Extending Identity and Access Management

This area deals mainly with identity management and access control solutions. The individual's identity has to be verified through trust means. The individual's authorization to access information is determined. Business rules for classifying information as well as determining controlled unclassified information (CUI) prescribe why access to the information is needed. Identity management is handled thorough Public Key Infrastructure (PKI) and common access cards (CAC). HSPD-12/FIPS-201 is being examined (this is the Home Security Presidential Directive 12 and a NIST publication). In addition, DoD and DNI are promoting ABAC (Attribute based access control) solutions.

> *"Task 8.1 Complete implementation and DoD-wide issuance of DoD's HSPD-12/FIPS-201compliant credential.*
>
> *Task 8.2 Conduct ABAC pilots to test the effectiveness of the ABAC approach in operational settings, as well as to confirm that the attribute set is robust."*

Focus Area 9: Advancing Information Sharing Enablers

This area focuses on enablers for network centric services strategy and the data strategy. The net centric services strategy promotes SOA-based shared services, and the data strategy promotes communities of interest (COI). In addition, efforts such as the Universal Core (U-Core) is standardizing a small, universal set of data elements and is leveraging COIs to develop data elements applicable to their mission. The definitions are stored and shared in the DoD's Metadata Registry.

> *'Task 9.1 Provide recommendation for evolving/enhancing the COI construct in support of information and data sharing.*
>
> *Task 9.2 Continue to develop and improve data standards for the exchange of basic information elements across the DoD enterprise*
>
> *Task 9.3 Establish business processes and funding models for implementing the Net Centric services strategy goals."*

Focus Area 10: Supporting DoD's Mission Needs Across Federal Information Sharing Initiatives

It is stated that as the DoD implements the information sharing strategy, it also has to coordinate and work with other federal agencies and their information sharing strategies. The example mentioned in the document include efforts by the National Command and Coordination Capability (NCCC), a White House directed program providing crisis management for the President and the Joint Continental US Communications Support Environment (JCCSE) Concept for Joint Command, Control, Communications and Computers (C4) that defines an approach for improving information sharing to support DoD missions of homeland defense supporting both defense and civil authorities.

> *"Task 10.1 Support as appropriate the FY 2010-2014 priorities for development of the federal ISE (Information Sharing Environment.)*
>
> *Task 10.2 When appropriate, support federal information sharing initiatives through consistent coordination and integration.*
>
> *Task 10.3 Develop a phased strategic level homeland defense civil support information sharing plan that captures information sharing processes, procedures, and critical information sharing requirements among key operation centers."*

In our research under the MURI project, we are addressing some of the focus areas. In particular, incentives for information sharing are a major goal. We are conducting experiments to show how incentives will enhance information sharing. In addition, the use of social networks to promote sharing is also being investigated. We are also conducting extensive research on policy-based information sharing and developing novel access control technologies for information sharing. Our infrastructure is based on semantic SOA that essentially integrates SOSA with semantic web technologies. Finally, we are conducting information sharing experiments among the team members as well as with our European partners (Kings College London, University of Insubria).

4. THE DEPARTMENT OF JUSTICE

4.1 Overview

One of the major concerns that came out of 9/11 was the lack of information sharing between the FBI (Federal Bureau of Investigation) and the CIA (Central Intelligence Agency). Since then, the Department of Justice has initiated several programs that promote information sharing within and across agencies. Notable among these efforts is the Justice Information Sharing program, which is a collection of initiatives, being

funded by the DOJ Office of Justice Programs.

Six prominent initiatives under Justice Information Sharing are the following:

- Global Justice Reference Architecture (JRA)
- National Information Exchange Model (NIEM)
- Justice XML
- Fusion Centers and Intelligence Sharing
- Security and Federated Identity Management
- Global Justice Information Sharing Initiative

In this section, we will address each of these initiatives and then discuss our solutions under the AFOSR funded projects relevant to these initiatives. Section 4.2 discusses JRA. NIEM is discussed in Section 4.3. Justice XML is discussed in Section 4.4. Fusion Centers are discussed in Section 4.5. Security issues are discussed in Section 4.6. Global Justice Information Sharing initiative is discussed in Section 4.7. Details on the DOJ information sharing initiatives can be found in the website of the DOJ Office of Justice Programs [DOJ].

4.2. Justice Reference Architecture

The Global Advisory Committee (GAC) of the Global Justice Information Sharing Initiative recommended the service-oriented architecture (SOA) model for the Justice reference architecture (JRA) which is based on the service-oriented paradigm. It is derived from the OASIS (Organization for the Advancement of Structured Information Standards) Reference Model for SOA 1.0. As stated in the JRA documentation,

> "JRA is an abstract framework for understanding significant components and the relationships between them within a Service-Oriented Architecture. It lays out common concepts and definitions as the foundation for the development of consistent SOA implementations within the justice and public safety communities."

The requirements of JRA included independence of information sharing partners, scalability, diversity of data source architecture, agility, reuse and sharing of assets and alignment with best practices and experience. JRA documentation also describes the service model for JRA, as well as service policy service contact and service agreement. More details on JRA can be found in [JRA].

DoDAF is the equivalent of JRA for the DoD. However, DoDAF was developed in the1990s, well before the SOA concepts. However, in mid 2000, DoDAF was architected for SOA. As we have stated earlier, our solution to promoting a federated information sharing approach is to share our research on federated information integration and policy management with the DoDAF community. Similarly, our research on developing a semantic event-based SOA for AISL can contribute to the JRA efforts.

4.3 Justice XML

The Global Justice Extensible Markup Language (XML) Data Model (Global JXDM) is an XML standard that has been adapted for representing and exchanging criminal justice information. It enables the law enforcement agencies, public safety agencies, prosecutors, public defenders and the judicial branch to share data effectively. The extent in the databases is represented in XML schema. This way heterogeneous database can be integrated efficiently.

It is stated that states such as Arizona, Pennsylvania, and Minnesota are adopting the Global JXDM into their information infrastructures and more than 50 law enforcement and justice-related projects have been implemented utilizing the Global JXDM. Some initiatives have adopted the key elements of the model, and have adapted it to meet their needs. More details on Justice XML can be found in [JUSTICE].

Like DoJ, DoD has also widely adopted XML for many of their information sharing efforts. For example, the DoD Metadata Registry is utilizing XML. Our research is focusing on technologies beyond XML. We are investigating the use of semantic web technologies such as RDF (Resource Description Framework) and OWL (Web Ontology Language) for representing and reasoning about information, This research is applicable for the needs of both the DoD and the DoJ.

4.4 National information Exchange Model

NIEM, the National Information Exchange Model, is a joint initiative between the DoJ and the DHS. As stated in the Justice Information Sharing program, the goal of the NIEM initiative is to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. NIEM builds on the Global Justice XML Data Model (GJXDM). NIEM and GJXDM initiatives enhance each others efforts. For example, GJXDM is used for NIEM implementation. The requirements developed by NIEM can be fed into the GJXDM initiative.

The components of NIEM include the following:

- Data components
- NIEM Core
- Domains
- Communities of Interest
- Information Exchange Package Documentation

Data components represent real-world concepts such as people, material, and places. Data components that are universally shared and understood are the universal components and for the NIEM Core. Domains add content and include Justice, Emergency Management, Immigration and International Trade. Communities of Interest (COIs) are collaborative groups that share goals and interests. Finally, the information exchanged is organized into Information Exchange Packets (IEP), which are implemented as XML schemas.

While DoJ and DHS have been developing NIEM since 2005, the DoD and the Intelligence community have been developing the Universal Core or UCore since 2007. UCore facilitates information sharing. It is based on CL schema and supports the National Information Sharing Strategy. Since NIEM and Ucore attempt to achieve similar objectives, the question is why not one model for information sharing? The NIEM/UCore partnership was subsequently formed to achieve multi-agency information sharing. The goal of this initiative was to share information between the justice, public safety, emergency- and disaster-management, intelligence, and homeland security communities. More details on NIEM can be found in [NIEM].

The AISL framework that we are developing can support the NIEM/UCore model. We provide a semantic infrastructure and associated services for information sharing. Our investigation goes beyond XML and brings in semantic web technologies for information representation and reasoning. We provide reasoning capabilities that are not possible with XML schemas.

4.5 Fusion Centers and Intelligent Sharing

As stated in the Justice Information Sharing website, a fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources. In addition, fusion centers are a conduit for implementing portions of the merging data from a variety of sources. In addition, fusion centers are a conduit for implementing portions of the *National Criminal Intelligence Sharing Plan* (NCISP). NCISP provides several needs for sharing criminal intelligence information and makes several recommendations for each of the needs. An example need is to:

> **"***identify an intelligence information sharing capability that can be widely accessed by local, state, tribal, and federal law enforcement and public safety agencies***."**

Two of the several recommendations to address the above need are:

> *(i) The CICC (Criminal Intelligence Coordination Council) shall work with Global's Systems Security Compatibility Task Force to identify and specify an architectural approach and transitional steps that allow for the use of existing infrastructures (technology, governance structures, and trust relationships) at the local, state, tribal, regional, and federal levels, to leverage the national sensitive but unclassified communications capabilities for information sharing. This strategic architectural approach shall ensure interoperability among local, state, tribal, regional, and federal intelligence information systems and repositories.*
>
> *(ii) Agencies are encouraged to utilize the latest version of the Global Justice Extensible Markup Language (XML) Data Model (Global JXDM) and its component Global Justice XML Data Dictionary (Global JXDD) when connecting databases and other resources to communication networks. The Global JXDM and Global JXDD were developed to enable interoperability through the exchange of data across a broad range of disparate information systems.*

While DOJ was developing plans for intelligence sharing and fusions centers, the Homeland Security Advisory Council (HSAC) Intelligence and Information Sharing Working Group was developing guidelines for local and state agencies for collecting, sharing and analyzing terrorism-related information. Subsequently, guidelines for fusion centers were developed for law enforcement, intelligence, public safety and the private sector. The goal is for law enforcement, private sector and public safety to work together to safeguard the nation. More details on Fusion Centers and Intelligence Sharing can be found in [FUSION].

In examining the needs of the National Criminal Intelligence Sharing Plan and the associated recommendations and comparing them with the DoD Information Sharing Strategy and Implementation Plan, there are many similarities. Both agencies are strongly promoting the establishment of governance structures as well as using standards for data representations. Therefore, the solutions we are developing for the DoD can be applied for the DoJ.

4.6 Security and Federated Identity Management

Information sharing involves placing trust on one's partners. Furthermore, appropriate security policies have to be enforced so that confidentiality of the information and privacy of the individuals are protected. In addition, the identity of the partners in a coalition has to be verified. The Global Federated Identity and Privilege Management (GFIPM) framework provides the justice community and partner organizations with a standards-based approach for implementing federated identity. To achieve GFIPM interoperability, we need globally understood metadata across federation systems. As stated in the GFIPM documentation, the GFIPM metadata and framework support the following:

- "*Identification/Authentication - Who is the end user and how were they authenticated?*
- *Privilege Management - What certifications, clearances, job functions, local privileges, and organizational affiliations are associated with the end user that can serve as the basis for authorization decisions?*
- *Audit - What information is needed or required for the purposes of auditing systems, systems access and use, and legal compliance of data practices?"*

The notion of "federation" is at the heart of the GFIPM framework. A *federation* is defined as a "group of two or more trusted partners with business and technical agreements that allow a user from one federation partner (participating agency A) to seamlessly access information resources from another federation partner (participating agency B) in a secure and trustworthy manner." Credential mechanisms are used to provide identity. GFIPM implements credentials in XML. The components of GFIPM are:

- Identity Provider (IDP)
- Service Provider (SP)
- User Credential Assertions (Metadata)

Within a federation, an organization could be an *identity provider* and/or a *service provider*. The identity provider verifies identity and handles account creation, provisioning, password management, and general account management. Service providers provide services such as child protection services and depend on the identity provider to validate the user requesting the service. Federation partners who offer services or share resources are known as service providers. The Global Security Group ensures that GFIPM is compatible with cross domain solutions such as NIEM. More details on security issues can be found in [GFIPM].

When comparing GFIPM with the DoD information sharing implementation plan, there are similar goals. In fact, Focus area 8 of the implementation states that identity management and access control have to be provided. Identity management will be implemented in accordance with HSPD-12/FIPS-201 and access control will be provided through ABAC. Our research on identity management and access control technologies will be applicable both to the DoD and to the DOJ communities.

4.7. Global Justice Information Sharing Initiative

The Global Justice Information Sharing Initiative is essentially an advisory committee to the Attorney General on information sharing and integration initiatives. This committee is one of the federal advisory committees (FAC). It prompts standards-based information sharing within the Justice community. It represents over 30 organizations which include members from law enforcement, judicial, and

correctional agencies. Details on the Global Justice Information Sharing Initiative can be found in [GLOBAL].

Associated with this initiative is GAC, the Global Advisory Committee that supports millions of justice professionals. Members of GAC include agency executives and policymakers, automation planners and managers, information practitioners, as well as end users. Through the Global Justice Information Sharing Initiative, information is exchanged and shared between the following people/agencies.

- Law enforcement agencies
- Prosecutors
- Public defenders
- Courts
- Correctional agencies
- Probation and parole departments
- Additional agencies directly involved in the justice process.

5. DEPARTMENT OF HOMELAND SECURITY

DHS published a document on its strategy for information sharing in April 2008. It is stated that the Intelligence Reform and Terrorism Prevention Act of 2004 ensured that DHS had a major role in the Information Sharing Environment (ISE) established by the President. The President subsequently established the Office of Program Manager for ISE (PM_ISE). In October 2007, the President initiated the development of the National Strategy for Information Sharing (NSIS). In addition, there was also an updated National Strategy for Homeland Security. Both strategies gave DHS a major role in information sharing at the national level. DHS also established an Information Sharing Coordinating Council, among many other activities. DHS then put out the following Transformation Statement:

> *"Transform DHS into an organization whose culture, business processes, and governance structure foster an information sharing environment that ensures the right information gets to the right people at the right time."*

The principles that guide the DHS information sharing strategy are the following:

- Fostering information sharing is a core DHS mission
- DHS must use established governance structure to make decisions regarding information sharing issues
- DHS must commit sufficient resources to information sharing
- DHS must measure progress toward information sharing goals
- DHS must maintain information and data security and protect privacy and civil liberties

The document states that while there are technological challenges, the major challenge in information sharing is establishing a process and developing protection mechanisms. Lack of trust is also a major challenge. Based on the challenges, DHS has put out its objectives for information sharing including the following:

1. *"Secure and maintain active participation in the ISE by each DHS component, directorate and office.*
2. *Fully coordinate DHS information policies, programs and projects with the ISE to promote sharing with Federal partners, while at the same time strongly advocating that the PM-ISE recognize and accommodate DHS mission needs, enterprise requirements and solutions.*

3. *Build a robust set of Shared Mission Communities to identify mission-specific information sharing opportunities and build trust, using the experience gained in establishing the Law Enforcement Shared Mission Community and in other endeavors.*
4. *Make the fusion centers an integral part of DHS and Federal information exchange with State, local, territorial, tribal and private sector partners.*
5. *Fully recognize and integrate federal, state, local, territorial, tribal, private sector and foreign government information needs as part of the DHS information sharing environment, consistent with applicable laws, regulations and international agreements.*
6. *Ensure that DHS technology platforms evolve to facilitate appropriate mission-based information sharing with federal, state, local, territorial, tribal, private sector and foreign partners.*
7. *Ensure that mission-relevant information sharing agreements are in effect with federal, state, local, territorial, tribal, private sector and foreign partners to promote information sharing consistent with the 'One DHS' mandate."*

DHS is involved in developing information sharing standards and protocols as well as appropriate security and privacy policies. DHS is also developing an approach to measure the performance of information sharing. In addition, DHS has produced a National Infrastructure Protection Plan (NIPP). This plan provides a risk management framework which is based on a public-private partnership that facilitates coordination within and across National Critical Infrastructure and key resources (CIKR). DHS also established the Information Sharing Network guided by NIPP and works in coordination with the ISE. In 2007, PM_ISE announced the adoption of CIKR ISE. CIKE ISE has a Capability Maturity Model and its five key components are:

- Coordination and governance
- Risk mitigation
- Relationship management
- Information exchange
- Content identification and development

DHS states that information sharing is an ongoing effort for them and has announced some new initiatives such as the Virtual US information sharing initiative announced in December 2009 and the Amtrak information sharing security initiative announced in July 2010 by the Secretary of DHS. Details on the DHS initiatives can be found in [DHS]. Our research on AISL will contribute towards the framework for information sharing for DHS including risk management and incentive aspects.

6. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

On February 22, 2008, the Director of National Intelligence published the US Intelligence Community's Information Sharing Strategy. It is stated in the report that "the inability or unwillingness to share information was recognized as an Intelligence Community weakness by both the 9/11 Commission and the Weapons of Mass Destruction (WMD) Commission. The report also states that since the findings of these commissions, the National Counterterrorism Center (NCTC) has stood up and the ISE was formed. The report addresses three major areas:

- Challenging new environment
- Information Sharing Strategy
- Implementation of the Strategy

The challenges include the changing and evolving threat, the need to transform the Intelligence Community, building an Integrated Intelligence Enterprise, and managing

risks. The Information Sharing strategy describes the new information model. Essentially, there is a need to migrate from:

(i) Need to Know to Responsibility to Provide
(ii) Agency Centric to Enterprise Centric
(iii) Static to Mission Centric
(iv) Network Centric to Information Centric
(v) Component-based to Attribute-based and
(vi) Data Owner to Data Stewardship.

The report then describes five strategic keystones for information sharing:

"Keystone #1: Intelligence Information Retrieval and Dissemination Moves Toward Maximizing Availability
Keystone #2: All Intelligence is Discoverable, and All Intelligence is Accessible by Mission
Keystone #3: Sharing Requires Greater Trust and Understanding of Mission Imperatives
Keystone #4: Developing a Culture that Rewards Information Sharing is Central to Changing Behaviors
Keystone #5: Creating a Single Information Environment (SIE) Will Enable Improved Information Sharing"

The keystones result in four major goals. These are:

Goal #1: Institute Uniform Information Sharing Policy and Governance
Goal #2: Advance Universal Information Discovery and Retrieval
Goal #3: Establish a Common Trust Environment
Goal #4: Enhance Collaboration Across the Community

The implementation strategy focuses on the following building blocks:

- Governance
- Policy
- Technology
- Culture
- Economics

The report also states that coordination is key to the Intelligence community. They recognize the need to coordinate their information sharing activities with those of the (i) National Strategy for Information Sharing (ii) DoD Strategy for Information Sharing, (iii) PM-ISE Information Sharing Environment implementation plan, (iv) Executive Office of the President, Office of Management and Budget Federal Enterprise Architecture (v) National Counterterrorism Center, (vi) National Counterintelligence Executive and (vii) National Intelligence Strategy Enterprise Objective 5. More details on this report can be found in [DNI].

In comparing the ODNI and DoD's Information Sharing Strategy, the implementation plans are closely aligned. Therefore, our research for the DoD is directly applicable to the ODNI with respect to policy, technology (e.g. SOS and information management), incentives, risk and cost for information sharing.

6. NATIONAL INFORMATION SHARING STRATEGY

Now that we have explained the information sharing strategies of the four major departments of the United States Government (e.g., DoD, DOJ, DHS, and IC), we will now discuss the National Information Sharing Strategy (NSIS) developed by the White House and published in October 2007. The administration felt that although information sharing had vastly improved since 9/11, there was an urgent need for a National Strategy to share terrorism- and law enforcement-related information at

multiple levels. In particular, the counterterrorism officials had the following needs.

- *Identify rapidly both immediate and long-term threats*
- *Identify persons involved in terrorism-related activities; and*
- *Implement information-driven and risk-based detection, prevention, deterrence, response, protection, and emergency management efforts.*

Therefore, a strategy to address the above needs at the national level was produced. The guiding principles of the strategy were the following:

- *"Effective information sharing comes through strong partnerships among federal, state, local, and tribal authorities, private sector organizations, and our foreign partners and allies;*
- *Information acquired for one purpose, or under one set of authorities, might provide unique insights when combined, in accordance with applicable law, with seemingly unrelated information from other sources, and therefore we must foster a culture of awareness in which people at all levels of government remain cognizant of the functions and needs of others and use knowledge and information from all sources to support counterterrorism efforts;*
- *Information sharing must be woven into all aspects of counterterrorism activity, including preventive and protective actions, actionable responses, criminal and counterterrorism investigative activities, event preparedness, and response to and recovery from catastrophic events;*
- *The procedures, processes, and systems that support information sharing must draw upon and integrate existing technical capabilities and must respect established authorities and responsibilities; and*
- *State and major urban area fusion centers represent a valuable information sharing resource and should be incorporated into the national information sharing framework, which will require that fusion centers achieve a baseline level of capability to gather, process, share, and utilize information and operate in a manner that respects individuals' privacy rights and other legal rights protected by U.S. laws."*

The five major components (called the guiding principles) of the strategy are the following:

- Information Sharing at the Federal Level
- Information Sharing with State, Local, and Tribal Entities
- Information Sharing with the Private Sector
- Sharing Information with Foreign Partners
- Protecting Information Privacy and Other Legal Rights

To share information at the federal level, NSIS has given NCTC the primary responsibility. The federal agencies that have terrorism-related information provide this information to NCTC. NCTC then analyzes and integrates the information. NCTC also serves as the shared terrorism-related knowledge base for the agencies. To share information with state, local and tribal governments, NSIS states that a culture of sharing has to be fostered. To support coordination at the multiple levels, the Interagency Threat Assessment and Coordination Group (ITACG), which is part of NCTC, was formed. ITACG's members include those from FBI, DHS and state and local representatives. In addition, State and Major urban fusion centers also coordinate gathering, analysis and dissemination of law enforcement, terrorism and public safety-related information. NSIS states that the majority of the nation's infrastructures are managed by the private sector. Therefore, information sharing among the public and private sectors is critical for national security.

Because terrorism is not limited to one nation and goes beyond borders, the US needs terrorism-related information from its coalition partners. Therefore, information sharing between US and international law enforcement agencies such as INTERPOL has to be carried out. NSIS also states that in all information sharing activities, the

privacy of the individuals is paramount. That is, only information pertaining to terrorism and law enforcement about an individual has to be shared. More details of the National strategy are given in [NSIS].

7. OTHER GOVERNMENT EFFORTS

Information sharing is critical for other organizations also including health care transportation, and energy applications. We briefly discuss some of the initiatives that have been proposed.

DOE has come up with information sharing policy for its Genomic data.

IRS states that its Fed/State Program saves government resources by partnering with state government agencies to enhance voluntary compliance with tax laws. This includes facilitating the exchange of taxpayer data, leveraging resources, and providing assistance to taxpayers to improve compliance and communications. IRS has answered several questions on its information sharing strategies to achieve its above goals.

DHHS agencies such as NIH and CDC have information sharing initiatives. For example, NIH has a program called "Clear Communication" whose objective is to "*cultivate a growing health literacy movement by increasing information sharing of NIH educational products, research, lessons learned, and research in the area of health literacy*".

DOT has created information sharing and analysis centers (ISAC) to share information related to protecting the various infrastructures.

8. INTERNATIONAL EFFORTS

International efforts including the effort of our coalition partners such as in the UK, Australia and Canada *have to be coordinated with the US strategies. In fact, the NSIS states that coordinating the activities with foreign partners is a major component of its strategy*. Transborder information sharing (e.g., US, Canada, Mexico), Transatlantic information sharing (e.g., US-EU) and Transpacific information sharing (e.g., US, Australia, Japan) are all important efforts.

Due to the Christmas Day 2009 Delta airline bomber incident, the US-EU transatlantic plan has been reviewed. A recent report commissioned by the Heinrich Böll Stiftung North America and the Migration Policy Institute (MPI) "*describes and analyzes the legal, privacy and data protection frameworks for information-sharing agreements relating to human mobility that enable the United States and the European Union to share such information for law enforcement purposes. It also examines the various informal and formal channels through which the United States and the European Union have discussed their privacy and personal data protection concerns.*" This report is titled *Transatlantic Information Sharing: At a Crossroads*. The recommendations offered by this report include [USEU]:

- "*The United States and the European Union should work toward negotiating a binding international agreement by setting up a roadmap that would help both sides lay out their goals and steps for diplomatic negotiations, while allowing relevant experts not involved in formal negotiations to offer their input.*

- *The U.S. government should consider establishing a central privacy office, helping assure European officials that the United States has an effective privacy watchdog. The United States and the European Union should update their respective privacy and personal data protection laws to reflect current security needs, and clearly define how those laws apply to citizens and noncitizens alike.*
- *The U.S. and E.U. governments should regularly provide public evaluations of the effectiveness of information-sharing agreements and the databases that collect and process information in stopping known or suspected terrorists and criminals from obtaining visas and entering their respective countries.*"

In July 2010, DHS Secretary Janet Napolitano and European VP for Justice Viviane Reding "vowed to work together to share data on terrorism and criminal investigations while safeguarding privacy of citizens on both sides of the Atlantic." One of the major challenges with this effort is the different policies and procedures enforced within US and EU. Furthermore, even within the US, the 50 states do not have uniform policies. The situation is worse within the EU countries. Even if the US-EU collaboration works, there are also several other factors such as the EU-Asia/Africa partnerships and the US-Pacific partnerships. Information sharing is a never-ending game. It will continue forever. We need to periodically review the progress made and the challenges encountered (e.g. the recent review of the US-EU information sharing strategy) and keep improving on the strategies and partnerships.

9. OUR ANALYSIS

Our analysis is given in the following bullets.

- One major observation for all 5 significant efforts (DoD, DHS, DOJ, IC, and White House) Incentives, Incentives, Incentives! for sharing are needed. This is stressed even more so for the sharing strategies of the DoD and Intelligence Community.
- Policy, Governance and Economics are also given a lot of consideration.
- Technology is important, but any solution must not depend on a particular technology. For example, SOA, XML and ABAC dominate at present. But this might change in the future.
- I believe that DoD and DOJ are leading the way.
- White House wants NCTC to coordinate the federal efforts.
- Each agency seems very committed to information sharing and has plans to share information within that agency. However, across agency collaboration and sharing, while significantly improved – e.g., NIEM-Ucore efforts between DOJ and DoD, the efforts are still stove piped.
- The role of NSIS (that at the White House level) is not clear. Also what is NSIS doing considering the fact that there has been a new administration since January 2009?
- Major players in information sharing are DoD, IC, DHS, DOJ and the White House. How can DOT, DHHS, DOE and Treasury be brought in to work with the major players?

- Cross domain solutions have to be given more consideration.
- Information sharing strategies should never end. It should be an on-going effort. The strategies should be updated as new events occur.
- Role of United Nations in global information sharing should be examined.

ACKNOWLEDGEMENT: This survey paper was carried out as part of the outreach efforts of the MURI project funded by AFOSR. The MURI team includes professors from UMBC, Purdue, UTD, UIUC, UTSA and U of MI.

REFERENCES

[AISL] http://aisl.umbc.edu/

[DHS] http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf

[DNI] http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf

[DOD1] http://cio-nii.defense.gov/sites/diea/InfoSharingStrategy.pdf

[DOD2] http://cio-nii.defense.gov/docs/DoD%20ISIP%20-%20APR%202009_approved.pdf

[DOJ] http://www.it.ojp.gov/default.aspx

[FUSION] http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181

[GFIPM] http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1179

[GLOBAL] http://www.iir.com/global/

[JRA] http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015

[JUSTICE] http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1013

[NIEM] http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1012

[NSIS] http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html

[USEU]http://www.boell.org/web/133-461.html